**UNITED STATES DISTRICT COURT**
**DISTRICT OF MASSACHUSETTS**

| | |
|---|---|
| *In re MAPFRE Data Disclosure Litigation* | Case No. 1:23-cv-12059-IT<br><br>**CONSOLIDATED CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiffs Lynne Alexandrowicz, Brian Conway, Fred Devereaux, Veronica Gregory, Richard Ma, Brian Ray, Annemarie Whilton (collectively, "MA Plaintiffs"), and David Brule (together with MA Plaintiffs, collectively referred to as "Plaintiffs"), individually and on behalf of all others similarly situated, by and through undersigned counsel, bring this class action complaint against Defendants MAPFRE U.S.A. Corp. (d/b/a MAPFRE Insurance) ("MAPFRE") and The Commerce Insurance Company ("Commerce," and together with MAPFRE, "Defendants") and allege as follows:

## I. INTRODUCTION

1. Every year, millions of Americans have their most valuable, highly sensitive personal information compromised by unauthorized individuals because corporations prioritize maximizing profits over protecting the sensitive information entrusted to them, leaving the public vulnerable to data disclosures and other data security incidents.

2. In recognition of the sensitivity of driver's license information (and its utility to identity thieves), Congress passed the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.* ("DPPA"), which restricts access to driver's license information, and mandates that private companies may only use that information for limited, enumerated purposes.

3. In the DPPA, Congress specifically defines personal information ("PI") to include driver's license numbers. *See* 18 U.S.C. § 2725(3). Thus, under the DPPA, private companies are

legally required to only access, or provide access to, driver's license numbers for very specific purposes.

4. Massachusetts also restricts access to driver's license information, and mandates that private companies may only use that information for limited, enumerated purposes. To access the information, companies must certify that they will "not use the information for any purpose not permitted under Massachusetts or Federal laws, rules or regulations … including the … DPP … [and] the Standards for the Protection of Personal Information of Residents of the Commonwealth … and will comply with such laws and Order and all other applicable laws, state or federal, regarding access to and the use of motor vehicle records, personal information and data privacy and protection."[1] Access is also contingent on agreement by the company that "Personal Information accessed under this Agreement shall not be used to create or aggregate the data for any purpose, except as specifically provided by federal or state law or other sections of this Agreement."

5. Massachusetts specifically defines Personal Information ("PI") to include driver's license numbers. *See* 201 CMR 17.02. Thus, under Massachusetts' law, private companies are legally required to only access, or provide access to driver's license numbers for specific purposes.

6. Threat actors seek out driver's license numbers because they are highly valuable pieces of PI. A driver's license number can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200.[2] Driver's license

[1] *See* COMM. OF MASS., "Agreement for Access to Records and Data Maintained by the Registry of Motor Vehicles," available at https://www.mass.gov/doc/dvs-packet-for-access/download (last accessed Apr. 8, 2024).

[2] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico In Months-Long*

numbers are particularly useful to identity thieves for applying for unemployment or other government benefits.

7. Defendants are providers of private passenger automobile insurance policies and offer coverages to automobile insureds throughout the United States. Defendants tout themselves as the 19th largest provider of automobile insurance in the United States.[3] Defendants market their insurance policies through the MAPFRE website, which contains an online quoting platform ("Quote Platform") through which prospective customers can apply for insurance coverage and receive a quote from Defendants online.

8. Despite knowing that driver's license numbers can only be used and disclosed for specific enumerated purposes, Defendants knowingly and willfully designed and implemented a feature on their Quote Platform where an individual's driver's license number would auto-populate in the Quote Platform or otherwise become viewable by the public—after only a bare minimum of publicly available information was entered about an individual (i.e., name, address, etc.)—making the auto-populated driver's license number visible to users of Defendants' Quote Platform, despite the fact that such users had no permissible purpose to access or view driver's license numbers under the DPPA and Defendants had no way to verify that those auto-populated driver's license numbers were shown to only the individuals to whom they belonged.

9. Defendants did so for their own self-interest: to increase the likelihood that consumers would complete their applications and purchase insurance policies from Defendants

---

*Breach*, Forbes (Apr. 20, 2021, 11:57 A.M. EDT), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=146576a68658.

[3] MAPFRE INSURANCE, https://www.mapfreinsurance.com/careers/our-company/#:~:text=MAPFRE%20Insurance%20is%20the%2019th,insurer%20in%20the%20United%20States (last visited Apr. 8, 2024).

through the Quote Platform. By automatically pulling information about consumers' driver's license numbers into the Quote Platform, Defendants sidestepped the process of asking Quote Platform visitors to fill in their driver's license numbers themselves. By limiting the amount of information such visitors needed to enter in order to receive an insurance quote—by pre-filling that information instead—Defendants reduced the time and effort required to complete the application process in order to sell more insurance, but at the cost of publicly displaying individuals' highly sensitive driver's license numbers.

10. Nothing about Defendants' underwriting or insurance quoting process required them to auto-populate driver's license numbers on their website. Indeed, Defendants had offered online insurance quotes to applicants long before they incorporated this auto-population feature to their Quote Platform; instead, Defendants added the auto-population feature to gain a competitive advantage in their sales process. That is, the less information requested from the prospective customer, the more likely they are to finish the application and purchase insurance from Defendants. Thus, Defendants' conduct was motivated by their desire to entice customers to complete applications for insurance.

11. By knowingly and intentionally designing and implementing the auto-population feature on their Quote Platform, Defendants knowingly and intentionally obtained, used, and disclosed Plaintiffs' and class members' driver's license numbers (and other PI) on their Quote Platform. Defendants' decision made driver's license numbers and PI easily accessible to anyone who entered a prospective customer's basic information.

12. Defendants designed their Quote Platform and website to display driver's license numbers and other PI to any website user who entered basic information about someone—even if it is not the person to whom the sensitive information relates. Defendants did not implement or

maintain any effective security processes or systems to prevent unauthorized parties and/or automated bots from using Defendants' website to harvest consumers' PI through their Quote Platform.

13. In essence, in their pursuit of selling more insurance and improving their bottom line, Defendants intentionally created a website that allowed anyone to look up someone's driver's license number and other PI, merely by entering rudimentary information about such a person. Defendants posted Plaintiffs' and the class members' driver's license numbers and PI on the internet's "windshield," for all digital passersby to see.

14. Unsurprisingly, Defendants' profit-seeking conduct quickly caught the attention of opportunists, who utilized Defendants' Quote Platform to obtain the highly sensitive driver's license numbers and PI of approximately 266,142 consumers, including Plaintiffs (the "Data Disclosure").[4]

15. Defendants sent letters to individuals impacted by the Data Disclosure beginning on or about August 22, 2023 (the "Notice"), stating that "[b]etween July 1 and July 2, 2023, an unknown party used information about you . . . to obtain access to additional information about you through MAPFRE's Massachusetts online quoting platform in Massachusetts."[5]

16. According to the Notice, unauthorized parties accessed and obtained driver's license numbers and other highly sensitive PI through Defendants' Quote Platform: "We have determined that the unknown party obtained access to your driver's license number through

[4] *See* COMM. OF MASS. OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, *Data Breach Notification Report*, at 76, https://www.mass.gov/doc/data-breach-report-2023/download (last visited Apr. 8, 2024).

[5] COMM. OF MASS. OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, *Data Security Incident Report of MAPFRE Insurance*, https://www.mass.gov/doc/assigned-data-breach-number-30358-the-commerce-insurance-company-mapfre-insurancer/download (last visited Apr. 8, 2024).

MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number."[6]

17. In the Notice, Defendants acknowledged that driver's license numbers and other PI accessed through the Data Disclosure can be used to conduct various forms of fraud and identity theft and urged impacted individuals to "remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity."[7]

18. Defendants' Notice conveniently omitted that the information, used by the unauthorized third parties to obtain Plaintiffs' and Class Members' driver's license numbers and PI from Defendants' Quote Platform, was simply their names, addresses, and other similar contact information publicly available (commonly referred to as "phone book" information) through a simple Google search or accumulated in databases and widely available on the internet.

19. Defendants' Notice explains that the Data Disclosure occurred on July 1-2, 2023, which means Defendants failed to discover—or inform Plaintiffs and Class Members of—the Data Disclosure for nearly two months.

20. Defendants sent Notices to Plaintiffs confirming that their sensitive driver's license numbers and PI were obtained by Defendants, displayed or otherwise disclosed on Defendants' website through the Quote Platform, and ultimately accessed by cybercriminals. Defendants use the Quote Platform to attract and obtain new business and increase their revenue and profit.

[6] *Id.*
[7] *Id.*

21. As a result of Defendants' intentional conduct in obtaining, using, and disclosing Plaintiffs' and Class Members' driver's license numbers and other PI on their Quote Platform for all to see, and the resulting Data Disclosure, Plaintiffs' privacy has been invaded, their sensitive driver's license information is now in the hands of unauthorized third parties, and they face a substantially increased risk of identity theft and fraud. Accordingly, Plaintiffs now must take immediate and time-consuming action to protect themselves from identity theft and fraud.

22. To redress Defendants' illegal, self-interested, profit-seeking conduct, Plaintiffs bring this class action on behalf of themselves and all other individuals ("Class Members") who had their driver's license numbers and other PI obtained by Defendants, displayed or otherwise disclosed on Defendants' website through the Quote Platform, used by Defendants to attract and obtain new business and increase their revenue and profit, and ultimately accessed by cybercriminals via the Data Disclosure. Plaintiffs, on behalf of themselves and the Class Members, seek remedies, including monetary damages and injunctive relief (including relief under the federal Declaratory Judgment Act), for negligence, invasion of privacy, and Defendants' violations of the DPPA and Massachusetts General Laws, Ch. 93.

## II. PARTIES

### A. Plaintiffs

23. Plaintiff Lynne Alexandrowicz is a resident and citizen of the Commonwealth of Massachusetts.

24. Plaintiff David Brule is a resident and citizen of the state of Arizona.

25. Plaintiff Brian Conway is a resident and citizen of the Commonwealth of Massachusetts.

26. Plaintiff Fred Devereaux is a resident and citizen of the Commonwealth of Massachusetts.

27. Plaintiff Veronica Gregory is a resident and citizen of the Commonwealth of Massachusetts.

28. Plaintiff Richard Ma is a resident and citizen of the Commonwealth of Massachusetts.

29. Plaintiff Brian Ray is a resident and citizen of the Commonwealth of Massachusetts.

30. Plaintiff Annemarie Whilton is a resident and citizen of the Commonwealth of Massachusetts.

**B. Defendants**

31. Defendant MAPFRE (formerly known as The Commerce Group, Inc.) is a domestic for-profit corporation organized under the laws of Massachusetts, with its principal place of business in Webster, Massachusetts. MAPFRE insures private passenger automobiles and provides homeowner and other types of insurance for qualified applicants. MAPFRE's affiliates are American Commerce Insurance Company (Columbus, Ohio); Citation Insurance Company (Webster, MA); The Commerce Insurance Company (Webster, MA); Commerce West Insurance Company (California COA No. 06715; San Ramon, CA): MAPFRE Insurance Company (California COA No. 18643; Florham Park, NJ); and MAPFRE Insurance Company of Florida (Miami, FL). MAPFRE obtained access to Plaintiffs' and Class Members' PI in the regular course of its business.

32. Defendant Commerce is a domestic for-profit corporation organized under the laws of Massachusetts, with its principal place of business in Webster, Massachusetts. Defendant

Commerce is a corporate subsidiary of MAPFRE responsible for underwriting automobile insurance policies sold and offered by MAPFRE.[8] Defendant Commerce obtained access to Plaintiffs' and Class Members' PI in the regular course of its business.

## III. JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 as it arises under the laws of the United States, including the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.*

34. This Court also has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a).

35. Alternatively, this Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and diversity exists because upon information and belief, at least one Class Member and Defendants are citizens of different states.

36. The Court has personal jurisdiction over Defendants because they maintain their headquarters and principal places of business in this District and conduct significant business in this District, thus availing themselves of Massachusetts' markets by selling auto insurance policies therein; they have sufficient minimum contacts with Massachusetts; and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District.

37. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because, *inter alia*, a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, were

[8] *See* https://www.universalhub.com/files/mapfreletter.pdf, at 1, footnote (last accessed Apr. 8, 2024).

directed to, and/or emanated from this District; Defendants transact substantial business and have agents in this District; a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District; and because Plaintiffs reside within this District.

## IV. FACTUAL ALLEGATIONS

### A. Plaintiffs' Experiences

#### i. *Plaintiff Lynne Alexandrowicz*

38. MAPFRE sent Plaintiff Alexandrowicz a letter dated August 24, 2023, informing her that MAPFRE disclosed her driver's license number and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

39. Prior to July 2023, Plaintiff Alexandrowicz never received a quote for a MAPFRE insurance policy, nor did she purchase one.

40. Plaintiff Alexandrowicz has spent considerable time and effort and taken (and continues to take) considerable precautions, to monitor for and protect against the unauthorized dissemination of her driver's license number and PI. To date, she has spent approximately 6 hours researching the breach, freezing her credit at all three credit bureaus, monitoring her accounts, and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing her PI, Plaintiff Alexandrowicz's sensitive PI was disseminated without her consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

41. Plaintiff Alexandrowicz is very careful about sharing her PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further,

Plaintiff Alexandrowicz stores documents containing her PI in a secure location and takes steps to ensure her online accounts are secure and password protected.

42. As a result of Defendants' Data Disclosure, Plaintiff Alexandrowicz has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of her disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PI; and injury to her privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Alexandrowicz now faces a substantial risk that unauthorized third parties will further misuse her PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and the unauthorized third parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Alexandrowicz has (1) suffered, or is at an increased risk of suffering, unauthorized use of her disclosed PI such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time she spent taking protective measures that would

have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Disclosure.

43. Plaintiff Alexandrowicz experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of her PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Alexandrowicz would compensate her for the foregoing redressable injuries. Further, Plaintiff Alexandrowicz seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

**ii. *Plaintiff David Brule***

44. MAPFRE sent Plaintiff Brule a letter dated October 19, 2023, informing him that MAPFRE disclosed his name, date of birth, driver's license number, and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

45. Prior to July 2023, Plaintiff Brule never received a quote for a MAPFRE insurance policy, nor did he purchase one.

46. Plaintiff Brule has spent considerable time and effort and taken (and continues to take) considerable precautions, to monitor for and protect against the unauthorized dissemination of his driver's license number and PI. To date, he has spent approximately 2-3 hours researching the incident, contacting MAPFRE, and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing his PI, Plaintiff Brule's sensitive PI was disseminated without his consent, is at high risk of being

fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

47. Plaintiff Brule is very careful about sharing his PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Plaintiff Brule stores documents containing his PI in a secure location and takes steps to ensure his online accounts are secure and password protected.

48. As a result of Defendants' Data Disclosure, Plaintiff Brule has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of his disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Brule now faces a substantial risk that unauthorized third parties will further misuse his PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and the unauthorized third parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Brule has (1) suffered, or is at an increased risk of suffering, unauthorized

use of his disclosed PI such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Disclosure.

49. Plaintiff Brule experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of his PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Brule would compensate him for the foregoing redressable injuries. Further, Plaintiff Brule seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

**iii. *Plaintiff Brian Conway***

50. In or about October 2023, MAPFRE sent Plaintiff Conway a letter informing him that MAPFRE disclosed his driver's license number and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

51. On or about August 24, 2023, MAPFRE sent Plaintiff Conway a letter informing him that MAPFRE disclosed his driver's license number and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

52. The notice letter stated that "[b]etween July 1 and July 2, 2023, an unknown party used information about you—which was already in the unknown party's possession—to obtain

access to additional information about you through MAPFRE's Massachusetts online quoting platform in Massachusetts." It further stated: "We have determined that the unknown party obtained access to your driver's license number through MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number."

53. Following the Data Disclosure, on or about September 2, 2023, Plaintiff Conway experienced an approximately $345.71 fraudulent charge on his Citi Mastercard. This fraudulent transaction is temporally and logically connected to the data derived from MAPFRE's Data Disclosure in the same way that data breach and other privacy cases have found to be "fairly traceable." MAPFRE disclosed Plaintiff Conway's driver's license number and PI shortly before he experienced this fraud.

54. Plaintiff Conway has spent and continues to spend considerable time and effort, and has taken and continues to take considerable precautions, to monitor for and protect against the unauthorized dissemination of his driver's license number and PI. To date, he has spent approximately 32 hours monitoring accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing his PI, Plaintiff Conway's sensitive PI was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

55. Plaintiff Conway is very careful about sharing his PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Plaintiff Conway stores documents containing his PI in a secure location and takes steps to ensure his online accounts are secure and password protected.

56. As a result of Defendants' Data Disclosure, Plaintiff Conway has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of his disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Conway now faces a substantial risk that unauthorized third parties will further misuse his PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and the unauthorized third parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Conway has (1) suffered, or is at an increased risk of suffering, unauthorized use of his disclosed PI such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Disclosure.

57. Plaintiff Conway experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of his PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Conway would compensate his for the foregoing redressable injuries. Further, Plaintiff Conway seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

**iv. *Plaintiff Fred Devereaux***

58. Plaintiff Devereaux signed up about 30 years ago to use Commerce Insurance, which was later acquired by MAPFRE. Plaintiff Devereaux terminated his Commerce Insurance policy approximately 5 years ago. In making the decision to entrust his Private Information decades ago, Plaintiff Devereaux relied upon basic privacy guarantees.

59. Prior to July 2023, Plaintiff Devereaux purchased a MAPFRE insurance policy.

60. MAPFRE sent Plaintiff Devereaux a letter dated August 24, 2023, informing him that MAPFRE disclosed his driver's license number and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

61. The notice stated: "unknown party obtained access to your driver's license number through MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number."

62. Plaintiff Devereaux has spent considerable time and effort and taken (and continues to take) considerable precautions, to monitor for and protect against the unauthorized dissemination of his driver's license number and PI. Since the breach, he has spent approximately

30 minutes each day monitoring his bank and brokerage accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing his PI, Plaintiff Devereaux's sensitive PI was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

63. Plaintiff Devereaux is very careful about sharing his PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Plaintiff Devereaux stores documents containing his PI in a secure location and takes steps to ensure his online accounts are secure and password protected.

64. As a result of Defendants' Data Disclosure, Plaintiff Devereaux has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of his disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Devereaux now faces a substantial risk that unauthorized third parties will further misuse his PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and the unauthorized third parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly

sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Devereaux has (1) suffered, or is at an increased risk of suffering, unauthorized use of his disclosed PI such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Disclosure.

65. Plaintiff Devereaux experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of his PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Devereaux would compensate his for the foregoing redressable injuries. Further, Plaintiff Devereaux seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

**v. *Plaintiff Veronica Gregory***

66. MAPFRE sent Plaintiff Gregory a letter dated August 22, 2023, informing her that MAPFRE disclosed her driver's license number and vehicle information to unauthorized third parties through MAPFRE's Quote Platform.

67. Plaintiff Gregory has spent considerable time and effort and taken (and continues to take) considerable precautions, to monitor for and protect against the unauthorized dissemination of her driver's license number and PI. To date, she has spent approximately 10 hours

monitoring accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing her PI, Plaintiff Gregory's sensitive PI was disseminated without her consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

68. Plaintiff Gregory is very careful about sharing her PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Plaintiff Gregory stores documents containing her PI in a secure location and takes steps to ensure her online accounts are secure and password protected.

69. As a result of Defendants' Data Disclosure, Plaintiff Gregory has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of her disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PI; and injury to her privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Gregory now faces a substantial risk that unauthorized third parties will further misuse her PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and the unauthorized third parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as

(*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Gregory has (1) suffered, or is at an increased risk of suffering, unauthorized use of her disclosed PI such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Disclosure.

70. Plaintiff Gregory experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of her PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Gregory would compensate her for the foregoing redressable injuries. Further, Plaintiff Gregory seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

**vi. *Plaintiff Richard Ma***

71. Plaintiff Ma signed up to use MAPFRE insurance in June 2018. In making the decision to entrust his PI to MAPFRE, Plaintiff Ma relied upon the data security services and privacy guarantees advertised by Defendants.

72. Prior to July 2023, Plaintiff Ma purchased a MAPFRE insurance policy.

73. MAPFRE sent Plaintiff Ma a letter dated August 24, 2023, informing him that MAPFRE disclosed his driver's license number and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

74. The notice stated: "unknown party obtained access to your driver's license number through MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number."

75. Since the announcement of the Data Disclosure, Plaintiff Ma has received frequent alerts that his PI has been found on the dark web. Additionally, he has been the victim of fraud: on or about December 25, 2023, he received a fraud alert that there were fraudulent or unauthorized charges on his debit card. Plaintiff Ma has been required to spend his valuable time and resources monitoring his financial accounts in an effort to detect and prevent misuses of his PII. Plaintiff Ma would not have to undergo such time-consuming efforts but for the Data Disclosure.

76. Plaintiff Ma has spent considerable time and effort and taken (and continues to take) considerable precautions, to monitor for and protect against the unauthorized dissemination of his driver's license number and PI. To date, he has spent approximately 7 hours researching the incident, monitoring accounts, and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing his PI, Plaintiff Ma's sensitive PI was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

77. Plaintiff Ma is very careful about sharing his PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Plaintiff Ma stores documents containing his PI in a secure location and takes steps to ensure his online accounts are secure and password protected.

78. As a result of Defendants' Data Disclosure, Plaintiff Ma has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of his disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Ma now faces a substantial risk that unauthorized third parties will further misuse his PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and the unauthorized third parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Ma has (1) suffered, or is at an increased risk of suffering, unauthorized use of his disclosed PI such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Disclosure.

79. Plaintiff Ma experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of his PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Ma would compensate his for the foregoing redressable injuries. Further, Plaintiff Ma seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

**vii. *Plaintiff Brian Ray***

80. Plaintiff Ray signed up to use MAPFRE insurance about 3 or 4 years ago. In making the decision to entrust his Private Information to MAPFRE, Plaintiff Ray relied upon the data security services and privacy guarantees advertised by Defendants.

81. Prior to July 2023, Plaintiff Ray purchased a MAPFRE insurance policy.

82. MAPFRE sent Plaintiff Ray a letter dated on or about August 2023 informing him that MAPFRE disclosed his driver's license number and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

83. Since the announcement of the Data Disclosure, Plaintiff Ray has been the victim of identity theft: he has experienced the fraudulent opening of several lines of credit in his name, which he found out by contacting one of the credit bureaus. Plaintiff Ray has been required to spend his valuable time and resources monitoring his financial accounts, changing passwords, and contacting the credit bureaus about a credit freeze in an effort to detect and prevent misuses of his PII. Plaintiff Ray would not have to undergo such time-consuming efforts but for the Data Disclosure.

84. Plaintiff Ray has spent considerable time and effort and taken (and continues to

take) considerable precautions, to monitor for and protect against the unauthorized dissemination of his driver's license number and PI. To date, he has spent multiple hours freezing his credit with all three credit bureaus, monitoring accounts, and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing his PI, Plaintiff Ray's sensitive PI was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

85. Plaintiff Ray is very careful about sharing his PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Plaintiff Ray stores documents containing his PI in a secure location and takes steps to ensure his online accounts are secure and password protected.

86. As a result of Defendants' Data Disclosure, Plaintiff Ray has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of his disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Ray now faces a substantial risk that unauthorized third parties will further misuse his PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the

type of PI Defendants disclosed and the unauthorized third parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Ray has (1) suffered, or is at an increased risk of suffering, unauthorized use of his disclosed PI such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Disclosure.

87. Plaintiff Ray experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of his PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Ray would compensate his for the foregoing redressable injuries. Further, Plaintiff Ray seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

**viii. *Plaintiff Annemarie Whilton***

88. MAPFRE sent Plaintiff Whilton a letter dated October 19, 2023, informing her that MAPFRE disclosed her driver's license number and vehicle(s) make(s), model(s), year(s), and vehicle identification number(s) to unauthorized third parties through MAPFRE's Quote Platform.

89. The notice letter stated that "[b]etween July 1 and July 2, 2023, an unknown party used information about you—which was already in the unknown party's possession—to obtain access to additional information about you through MAPFRE's Massachusetts online quoting platform in Massachusetts." It stated further: "We have determined that the unknown party obtained access to your driver's license number through MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number."

90. A week after the start date of the Data Disclosure (i.e., July 1, 2023), Plaintiff Whilton discovered that her PI was used to submit a fraudulent claim for unemployment benefits in her name in Massachusetts.

91. Specifically, on or about July 5, 2023, Plaintiff Whilton attempted to apply for unemployment benefits on the designated Massachusetts' agency website, but received an error message informing her that the online system would not accept her PI because it was linked to another individual who had submitted a claim for unemployment benefits in Plaintiff Whilton's name. Thus, Plaintiff Whilton's PI has been used to commit fraud in her name. On the application page of that website, it displayed Plaintiff Whilton's name and social security number, but listed someone else's email address and phone number as being linked to her even though they were not her own.

92. Extremely alarmed and stressed by the discovery—and to investigate and troubleshoot the fraud—Plaintiff Whilton immediately drove to the Quincy, Massachusetts Unemployment Office to attempt to apply for unemployment benefits in person. Plaintiff Whilton was forced to wait 3-4 hours before being able to speak with an employee at the Quincy office, only for that employee to inform her that she needed to go to the Massachusetts Social Security

Administration Office located in Quincy, Massachusetts. Plaintiff Whilton then drove to that second office where she waited for an additional 1-2 hours before being able to meet with an employee who told her that she needed to contact the Boston Police and visit the Boston Office for Unemployment Assistance. Plaintiff Whilton then traveled to the Boston Office for Unemployment Assistance located in Boston, Massachusetts where she waited for approximately 3 hours. Plaintiff Whilton was also instructed to contact Program Integrity about the incident, which she did multiple times. Every entity that Plaintiff Whilton contacted was unable to help her and would direct her to a different entity, which was extremely stressful and time consuming.

93. While at the Commonwealth of Massachusetts Department of Unemployment Assistance, Plaintiff Whilton submitted a Fraud Reporting Form to formally report that a claim for unemployment benefits was fraudulently submitted in her name. In response, Plaintiff Whilton received an email from the Commonwealth of Massachusetts Department of Unemployment Assistance on or about July 6, 2023, stating: "Unfortunately, if an unemployment claim was fraudulently filed using your name … you were likely the victim of an earlier national or private sector data breach. It is likely that these criminal enterprises were in possession of your [PI] in order to file a fraudulent claim." The letter made clear that the fraudulent claim for unemployment benefits in her name exposed Plaintiff Whilton to a substantial risk of further fraudulent misuse of her PI, as well as identity theft and further future harm:

> Given the potential larger impact to you, we suggest you take steps to protect yourself and your information, including:
>
> 1. File a police report with your local police department. Get a copy of the report that you can provide to creditors and credit agencies.
> 2. Change passwords on your email, banking, and other personal accounts.
> 3. Make a list of credit card companies, banks, and other financial institutions where you do business. Tell them you are a victim of identity theft and ask them to put a fraud alert on your account.

4. Get a copy of your credit report and dispute any fraudulent transactions. You can request credit reports online from the 3 major credit reporting agencies (Equifax, Experian, and Transunion) or by calling (877) 322-8228.
5. Place a credit freeze with each of the 3 major credit reporting agencies. Call each of the credit reporting agencies at these phone numbers or visit their websites to freeze your credit ….
6. Place a fraud alert on your credit file. You can do this by contacting just 1 of the credit agencies to add an alert with all 3 agencies.
7. Notify your employer.
8. Tell the National Center for Disaster Fraud
9. Take notes about all conversations and keep copies of all records.

94. Because Plaintiff Whilton was unable to submit a claim for unemployment benefits due to a fraudulent claim being submitted in her name, on or about July 10, 2023, Plaintiff Whilton filled out and submitted a Request to Update Multi-Factor Authentication Information in UI Online, at the Commonwealth of Massachusetts Department of Unemployment Assistance located in Boston. That form required Plaintiff Whilton to provide her Massachusetts driver's license number, indicating that—upon information and belief—Massachusetts driver's license numbers are required for applications for, and/or administration of, unemployment benefits.

95. All of the foregoing prevented Plaintiff Whilton from receiving unemployment benefits for approximately seven weeks, during which Plaintiff Whilton continued to spend time and energy troubleshooting the issue.

96. On October 6, 2023, Plaintiff Whilton experienced fraudulent charges on her Discover credit card in the amount of $170. Plaintiff Whilton contacted Discover multiple times to inquire about and dispute these charges, which Discover ultimately reimbursed in full. Because of these fraudulent charges, Plaintiff Whilton now regularly spends extra time that could have been spent on more productive things monitoring all of her financial accounts for fraudulent charges.

97. Plaintiff Whilton has spent considerable time and effort and taken (and continues to take) considerable precautions, to monitor for and protect against the unauthorized dissemination of her driver's license number and PI. To date, she has spent approximately 20-30

hours troubleshooting the two separate incidents of fraudulent misuse of her PI alleged above, and otherwise monitoring accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing her PI, Defendant disclosed Plaintiff Whilton's sensitive PI without her consent, which places her at high risk of having her PI fraudulently misused by unauthorized third parties, and the value of that information was quantifiably reduced.

98. Plaintiff Whilton is very careful about sharing her PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Plaintiff Whilton stores documents containing her PI in a secure location and takes steps to ensure her online accounts are secure and password protected.

99. As a result of Defendants' Data Disclosure, Plaintiff Whilton has suffered—or is at an increased risk of suffering—injury and/or damages, including but not limited to, the unauthorized use of her disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PI; and injury to her privacy. Additionally, because of Defendants' Data Disclosure, Plaintiff Whilton now faces a substantial risk that unauthorized third parties will further misuse her PI. Indeed, because (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through its Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and the unauthorized third

parties obtained in the Data Disclosure—i.e., mainly driver's license numbers—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (inter alia) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts, Plaintiff Whilton has (1) suffered, or is at an increased risk of suffering, unauthorized use of her disclosed PI such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Disclosure.

100. Plaintiff Whilton experienced all of the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of her PI in the Data Disclosure. The monetary relief sought herein by Plaintiff Whilton would compensate her for the foregoing redressable injuries. Further, Plaintiff Whilton seeks injunctive relief to redress the foregoing injuries and harm, including but not limited to requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

### B. Defendants Collect Vast Amounts of Sensitive PI from Consumers and Third Parties

101. Defendants primarily offer private passenger automobile and home insurance to individuals in 100 countries, including throughout the United States of America.[9] Defendants also

[9] *See* MAPFRE INSURANCE, *Who We Are*, https://www.mapfreinsurance.com/who-we-are/ (last visited Apr. 8, 2024).

insure motorcycles, sport bikes, cruisers, mopeds, scooters, touring bikes, dirt bikes, and other recreational and specialty vehicles.[10]

102. Defendants collect and store vast amounts of PI and sensitive data from prospective clients, current and former customers, and other consumers, as part of their regular business practices, including highly sensitive driver's license numbers, as well as names, aliases, postal addresses, Social Security numbers, bank account numbers, credit card numbers, medical information, protected classification characteristics, fingerprints, faceprints, voiceprints, iris scans, sleep data, exercise data, internet browsing and search history, geolocation data including physical location, job history, job performance evaluations, educational transcripts, student identification codes, psychological trends, predispositions, intelligence, and aptitudes.[11] Discovery will show that during the insurance claims process, Defendants also require submission of similar PI in connection with insurance processing claims, including from individuals who are not Defendants' policyholders but who are involved in a claim being handled by Defendants, such as drivers involved in accidents with Defendants' insureds.

103. Defendants' marketing is primarily through direct response methods in which consumers submit applications for insurance quotes directly to Defendants via the internet or by telephone, and to a lesser extent, through captive agents.

104. Competition for private passenger automobile insurance, which is substantial, tends to focus on price and level of customer service provided.

[10] *See* MAPFRE INSURANCE, *Motorcycle Insurance*, https://www.mapfreinsurance.com/motorcycle-insurance/ (last visited Apr. 8, 2024).
[11] *See* MAPFRE INSURANCE, *California Privacy Notice*, https://www.mapfreinsurance.com/getprivacypolicy/?lang=EN (last accessed Apr. 8, 2024).

105. Like other insurance providers, Defendants have an online Quote Platform available to all persons capable of accessing it via the internet. Visitors to Defendants' Quote Platform can get a quote instantly after providing basic PI.

106. Defendants' quoting feature uses the information entered by the website visitor, combined with additional information Defendants have or that Defendants can access from third-party data brokers, and then automatically displays the additional information to the visitor as part of the quote process.

107. Specifically, Defendants' quoting feature asks any visitor to the site for their name, date of birth, and address. Once a visitor enters that information, Defendants' system auto-populates the quotation with driver's license information from Defendants' own databases or from third-party prefill services and makes that information visible to the person entering the information on the Defendants' Quote Platform. A person's name, date of birth, and address are data that are often easily obtained. Defendants knew that this information was often available to the public at no cost, and that cybercriminals are commonly in possession basic data combinations, including name, address and date of birth.[12]

108. Given that Defendant's website functioned as a driver's license lookup too, scammers used an automated process on Defendant's instant Quote Platform to harvest Plaintiffs' and Class Members' driver's license numbers.

[12] For example, "[s]ince approximately 2009, MyLife has purchased public record data about individuals from data brokers. … MyLife uses that data to create a 'public listing' or profile for these individuals, which can be accessed through its website, www.mylife.com. … On its website, MyLife has profiles purporting to cover at least 320 million individuals. ... Information that may be available through a *free search may include: name; city and state of residence; … email address, and mailing address associated with the profile; date of birth*; …." *United States v. MyLife.com, Inc.*, No. CV 20-6692-JFW(PDX), 2021 WL 4891776, at *2 (C.D. Cal. Oct. 19, 2021) (citations omitted) (emphasis added).

109. The proposed Class includes many people who never applied for insurance with Defendants, were not Defendants customers, and may not even have been aware of Defendants' existence. In other words, unauthorized parties availed themselves of the PI Defendants made publicly available via their instant Quote Platform on a wholesale basis.

110. Defendants' Quote Platform did not require verification that the person or automated process accessing the system was actually the individual for whom the information was being entered. In addition, Defendants' Quote Platform did not employ effective, industry-standard security measures to detect whether the website visitor was, in fact, a "bot" or automated process rather than an individual person. Instead, Defendants knowingly and intentionally configured their online Quote Platform to provide PI—including driver's license numbers—when anyone, including bots, just entered basic information such as a person's name, date of birth, and address. Thus, Defendants' Quote Platform was purposefully and knowingly set up to allow any site visitor, including bots, to access and view PI including driver's license numbers of anyone about whom Defendants had collected or could access that PI simply so that Defendants could more easily sell their main product.

### C. Defendants Contravened the Purpose of the Driver's Privacy Protection Act

111. Prior to the enactment of the DPPA, Congress found that most states freely turned over DMV information to whomever requested it with few restrictions. 137 Cong. Rec. 27,327 (1993).

112. Due to this lack of restrictions, Congress grew concerned that potential criminals could easily obtain the private information of potential victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

113. These concerns did, in fact, materialize in the occurrence of crime, harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca Schaeffer, an upcoming actor,

after obtaining her unlisted home address from the California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA, Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

114. In response to public outrage over the Schaeffer murder and growing concern for the threat to public safety that free access to DMV records posed, Congress enacted the DPPA "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government." S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

115. Additionally, in enacting the DPPA, Congress was motivated by its "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released – even sold – with resulting loss of privacy for many persons." *Akkawi v. Sadr*, No. 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at *4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The release of private information like driver's license numbers and other motor vehicle records was the exact impetus for the DPPA's passage.

116. Congress sought to expressly prohibit "disclosing personal information obtained by the department in connection with a motor vehicle record." *Chamber of Com. of United States v.*

*City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). Driver's license numbers are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1), (3). As such, Congress used its lawmaking authority to properly elevate the disclosure driver's license numbers and other motor vehicle records into a concrete harm, a harm that bears a sufficiently close relationship to the tort of public disclosure long recognized at common law.

117. By knowingly using the PI of Plaintiffs and the Class for sales and marketing purposes, and by knowingly disclosing that PI to the public, Defendants ran afoul of the purpose of the DPPA, and threatened the privacy and safety of licensed drivers, for whose protection the statute was enacted. Defendants' actions constituted a concrete injury and particularized harm to Plaintiffs and members of the Class, that would not have happened but for Defendants' failure to adhere to the DPPA. Plaintiffs were harmed by the public disclosure of their PI in addition to the other harms enumerated herein.

**D. The Data Use and Disclosure, and Its Impact**

118. In its Notice, Defendants informed consumers that their sensitive PI—namely, driver's license numbers—was compromised in a security incident, which it described as follows:

> We have determined that the unknown party obtained access to your driver's license number through MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number.[13]

119. While the Notice indicates that "as soon as MAPFRE became aware of the issue, [we] took down our Massachusetts online quoting platform and conducted an investigation to determine what happened [and] implemented additional controls within our system to protect

[13] COMM. OF MASS. OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, https://www.mass.gov/doc/assigned-data-breach-number-30358-the-commerce-insurance-company-mapfre-insurancer/download (last accessed Apr. 8, 2024).

against a reoccurrence of the incident," the Notice does not provide the date when Defendants learned of or "became aware of" the incident. Instead, the Notice merely states that Defendants "determined" that the incident had occurred and provides no further details.[14]

120. Defendants' use of the driver's license numbers, their Data Disclosure through their online sales platform, and their violation of the law—including the DPPA—assisted an ongoing and concerted campaign by fraudsters to engage with insurers' Quote Platforms to obtain driver's license numbers.

121. On February 16, 2021, the New York State Department of Financial Services ("DFS") issued an alert regarding an ongoing systemic and aggressive campaign to engage with public-facing insurance websites—particularly those that offer instant online automobile insurance quotes like Defendants' website—to obtain non-public information, in particular unredacted driver's license numbers.[15] According to the alert, the unauthorized collection of driver's license numbers appeared to be part of a growing fraud campaign targeting pandemic and unemployment benefits. DFS first became aware of the campaign when it received reports from two auto insurers in December 2020 and January 2021 that cybercriminals were targeting their websites that offer instant online automobile insurance quotes to obtain unredacted driver's license numbers.

122. Insurers' instant online auto quoting websites are the primary entry point for cybercriminals to access consumers' PI. As the industry has accelerated adoption of faster-quoting processes and tools to achieve competitive advantage, new vulnerabilities have opened.[16] According to DFS, insurers noticed an unusually high number of abandoned quotes or quotes not

[14] *Id.*
[15] N.Y. DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn (last visited Apr. 8, 2024).
[16] *Id.*

pursued after the display of the estimated insurance premium. On the instant quote websites, "criminals entered valid name, any date of birth and any address information into the required fields" and "then displayed an estimated insurance premium quote along with partial or redacted consumer [PI] including a driver's license number. The attackers captured the full, unredacted driver's license numbers without going any further in the process and abandoned the quote."[17] Of course, Defendants need not use driver's license numbers on a sales platform, or disclose this information to the public, to underwrite any auto insurance policy.

123. In January 2021, DFS alerted approximately a dozen entities maintaining such websites that they were likely targets of unauthorized third-parties looking to gain access to New Yorkers' PI, specifically driver's license numbers. Following the alert, six more insurers apparently reported to DFS the malicious targeting of their websites—two of which insurers reported that the fraudsters failed to gain access to PI, and four of which reported that the fraudsters did gain access to PI or that their investigation was still ongoing. In the alert, DFS did not name the websites affected or the insurers.

124. The DFS issued a second alert on March 30, 2021, urging companies like Defendants to avoid displaying prefilled driver's license numbers "considering the serious risk of theft and consumer harm."[18]

125. The increase in interest in driver's license numbers is, in part, a product of the changes brought on by the COVID-19 pandemic, as various types of financial transactions that used to be conducted exclusively in person have been transferred online. Some states are also allowing residents to use expired driver's licenses for various purposes for an extended period, due

[17] *Id.*

[18] N.Y. DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Mar. 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup.

to difficulty in securing the in-person DMV appointments necessary to renew them.[19]

126. Unsurprisingly, fraudulent unemployment claims spiked during the pandemic, as more money became available to displaced workers and the requirements for filing eased. Many states even paid out tens of millions of dollars to scammers, a phenomenon largely driven by the unauthorized use of fraudulently obtained PI. Threat actors have been caught using not just sensitive personal data for these fraudulent unemployment claims, but also hacking into existing unemployment accounts to change bank payment information.[20]

127. The United States Department of Labor estimates that pre-pandemic fraudulent unemployment claims accounted for about 10% of all filings.[21] A normal yearly cost for fraudulent unemployment claims is about $3 billion; recent reports indicate that this number ballooned to $200 billion during the pandemic. Fraudulent first-time claims drove a lot of this activity, but experts expect the problem to persist even as most Americans head back to work. Some will fail to notify the state unemployment office of their change in employment status, creating an opening for scammers.

128. Defendants knew that they were using driver's license information on their online sales platform. Defendants also knew that this platform was created and maintained in a way that allowed fraudsters to plug in readily, publicly available basic PI of other persons, and that the website would auto-populate driver's license information once that basic information was entered.

---

[19] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Apr. 8, 2024).

[20] *Id.*

[21] Megan DeMatteo, *Unemployment fraud costs victims $200 billion annually in the U.S. – here's how to protect yourself*, CNBC (Dec. 3, 2023), https://www.cnbc.com/select/how-to-protect-yourself-from-unemployment-fraud/ (last visited Apr. 8, 2024).

Indeed, Defendants were responsible for their Quote Platform, including its design and design features. Defendants thus knew or should have known, that their website and the website's auto-populate feature disclosed consumers' driver's license number to unauthorized third parties. This is exactly how Defendants designed their website to operate. Not only did Defendants know that they were using driver's license numbers to sell insurance, and that they were disclosing driver's license numbers to the public, but they also failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumers' PI, and failed to implement basic safeguards to protect the security, confidentiality, and integrity of that information. By adding the auto-population feature to their Quote Platform, which Defendants knowingly and intentionally chose to do, Defendants intended to use the driver's license numbers and make the returned information easily accessible to anyone who entered basic information into their system. Defendants did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. Defendants did not impose effective security protocols to prevent automated bots from accessing consumers' PI. Thus, Defendants knowingly used and posted consumers' driver's license numbers directly to all members of the public.

### E. Defendants Acknowledged That the Use of Data and Their Data Disclosure Created a Substantial Risk of Identity Theft and Fraud

129. The extent, scope, and impact of Defendants' use of the data and their Data Disclosure on their customers and other consumers remains uncertain. Nevertheless, the harm caused to Plaintiffs and Class Members by Defendants' use of the information and their Data Disclosure is already apparent. Criminals now possess Plaintiffs' and Class Members' driver's license numbers, and their only purpose in obtaining and possessing that information is to monetize that data by selling it on the darknet or dark web or using it to commit other types of fraud.

130. Defendants' Notice puts the burden on Plaintiffs and Class Members to take

mitigating steps to protect their information: "We encourage you to remain vigilant against incidents of identity theft and fraud, and to monitor your free credit reports for suspicious activity and to detect errors. Enclosed with this letter are some steps you can take to protect your information[,]" and explains how to obtain one's credit reports, including initiating a credit freeze, checking the consumer's credit report, and enrolling in identity theft insurance.[22]

131. Having received the Notice about this Data Disclosure, it is reasonable for Plaintiffs and Class Members to believe that the risk of future harm (including identity theft or fraud) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. Defendants' specific instructions and warnings in the Notice relate to the fact that threat actors take driver's license numbers for the purpose of committing fraud in the name of the person whose license number is taken.

### F. The PI Defendants Obtained, Used and Then Disclosed in Their Data Disclosure Is Highly Valuable to Fraudsters

132. It is well known amongst companies that store or have access to sensitive PI that driver's license numbers are valuable and frequently targeted by criminals. The PI that Defendants voluntarily disclosed via their Quote Platform in violation of state and federal law is very valuable to phishers, identity thieves, cyber criminals, and other fraudsters, especially as an unprecedented numbers of criminals are filing fraudulent unemployment benefit claims, and driver's license information is uniquely connected to the ability to file such claims and commit other financial fraud. Unsecured sites that contain or transmit PI like driver's license numbers require notice to

[22] COMM. OF MASS. OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, https://www.mass.gov/doc/assigned-data-breach-number-30358-the-commerce-insurance-company-mapfre-insurancer/download (last accessed Apr. 8, 2024).

consumers when the data is stolen because it can be used to commit identity theft and other types of fraud.

133. The driver's license numbers disclosed in Defendants' Data Disclosure are significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. By contrast, the information disclosed in Defendants' Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, or to take out loans, especially student loans. The driver's license numbers disclosed in Defendants' Data Disclosure are also more valuable because they are long lasting, and difficult to change.

134. With access to an individual's driver's license number, criminals can commit all manner of fraud, including: obtaining government benefits in the victim's name, filing fraudulent tax returns using the victim's information, or obtaining a driver's license or official identification card in the victim's name but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name, and may even give the victim's driver's license number during an arrest, resulting in an arrest warrant being issued in the victim's name.[23] They can also use the driver's license when receiving a ticket or to provide to an accident victim, to replace or access account information on social media sites, to obtain a mobile phone, to dispute or approve a SIM swap, to redirect U.S. mail, to gain unauthorized access to the United States, to claim a lost or stolen passport, to use as a baseline to obtain a Commercial Driver's License, or to engage in phishing or other social engineering scams.

135. Fraudsters often aggregate information taken from data security incidents to build

[23] *See* FEDERAL TRADE COMMISSION, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited on Apr. 8, 2024).

profiles on individuals. These profiles combine publicly available information with information discovered in previous data security incidents and exploited vulnerabilities. Unique and persistent identifiers such as Social Security numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to forging an identity. When not all information is available, the information that is stolen is used to socially engineer a victim into providing additional information so a "full"[24] profile can be obtained.

136. There is no legitimate or legal reason for anyone to use Defendants' website to acquire driver's license information on Plaintiffs and the Class Members. Dark Net Markets ("DNM(s)"), or the "dark web," is a heavily encrypted part of the internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity. When malicious actors obtain ill-gotten PI, that information often ends up on the dark web because the malicious actors buy and sell that information for profit.[25] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

137. Any non-public data, especially government issued identification numbers like a driver's license or non-driver's identification number, has criminal value.[26] For example, a fake

[24] "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information for an entity or individual.

[25] IDENTITY FORCE, *Shining a Light on the Dark Web with Identity Monitoring*, Feb. 1, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Apr. 8, 2024).

[26] IDENTITY THEFT RESOURCE CENTER, *Can Someone Steal Your Identity From Your Driver's License?*, Feb. 19, 2021, https://www.idtheftcenter.org/can-someone-steal-your-identity-from-your-drivers-license/ (last visited Apr. 8, 2024).

U.S. citizenship kit for sale—passport, Social Security Number, driver's license, and birth certificate—is offered on the dark web for 0.218 bitcoin (or $1,400 at the time) and a stolen/fake driver's license (by U.S. state) for $200.[27]

138. In some ways, driver's license numbers are even more attractive than Social Security numbers to threat actors and more dangerous to the consumer when disclosed. Unlike a Social Security number, a driver's license number is not monitored as closely, so it can potentially be used in ways that will not immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend immediate notice and replacement, and that identity theft protections are put in place for a minimum of 3 years. Most cybersecurity experts, including Enterprise Knowledge Partners, recommend five years or more.

139. Blogger Gayle Sato from the national credit reporting company Experian emphasized the value of driver's license information to thieves and cautioned:

> Your driver's license may not seem like a jackpot for thieves, but it can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks. Worse, if your license data has been stolen in a data breach, you may not even know it's being misused.[28]

140. In fact, according to the data privacy and cyber security publication CPO Magazine:

---

[27] Daniel Shkedi, *Heart of Darkness: Inside the Darknet Markets that Fuel Financial Cybercrime*, BIOCATCH, https://web.archive.org/web/20210905231044/https://www.biocatch.com/blog/financial-cybercrime-darknet-markets (last visited Apr. 8, 2024).

[28] Gayle Sato, *What Should I Do If My Driver's License Number Is Stolen?*, EXPERIAN (Nov. 3, 2021) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Apr. 8, 2024).

> To those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: ". . . It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email."[29]

141. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application:

> Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver's license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name.[30]

142. The use of stolen driver's license numbers to obtain unemployment benefits under another person's name was confirmed by the New York State DFS on February 16, 2021, in its industry letter described above, which stated that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [PI,

---

[29] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Apr. 8, 2024).

[30] Zach Whittaker, *Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TECHCRUNCH (Apr. 19, 2021), https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name (last visited Apr. 8, 2024).

including] websites that provide an instant quote …. [and that] DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits."[31]

143. The process that was used to extract the data from Defendants' website was likely automated. The identity thieves have demonstrated the value they place on the driver's license numbers by engaging in a systematic and businesslike process for collecting them from Defendants' Data Disclosure and from additional insurers' websites offering instant quotes.

144. The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that, when criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name, this type of identity fraud can be the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime.[32] The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[33]

**G. Defendants Failed to Comply with Federal Trade Commission Requirements**

145. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and knowing disclosures of information via public websites, and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses

---

[31] N.Y. DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn (last visited Apr. 8, 2024).

[32] *See* UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, June 2007, http://www.gao.gov/assets/270/262899.pdf (last accessed Apr. 8, 2024).

[33] *Id.*

highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[34]

146. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[35] Among other things, the guidelines note businesses should properly dispose of PI that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[36]

147. Also, the FTC recommends companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[37]

148. Highlighting the importance of protecting against these types of disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against

---

[34] FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, June 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Apr. 8, 2024).

[35] *See* FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, Oct. 2016, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Apr. 8, 2024).

[36] *Id.*

[37] *Start With Security*, *see supra* n.35.

unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[38]

149. Through negligence in designing and implementing their online quoting platform and securing Plaintiffs' and Class Members' PI, Defendants knowingly allowed the public—and thieves—to utilize their online Quote Platform to obtain access to and collect individuals' PI. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiffs' and Class Members' PI. Defendants' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801.

### H. Plaintiffs' Injuries: Attempts to Secure PI After Defendants' Data Disclosure

150. Defendants admitted in the Notice that there was disclosure of Plaintiffs' and Class Members' driver's license numbers to unauthorized third parties. Defendants also concede that this disclosure created imminent harm to Plaintiffs and Class Members, specifically acknowledging that the Data Disclosure can lead to "incidents of identity theft and fraud." MAPFRE tasked Plaintiffs and Class Members with various mitigation steps and offered a year of credit monitoring. These measures are woefully inadequate and do not absolve Defendants of their violations of the DPPA and other laws alleged herein.

151. Plaintiffs and Class Members have been, and will continue to be, injured because Defendants disclosed their PI, and—per Defendants' instructions— they are now forced to spend

[38] *See* FEDERAL TRADE COMMISSION, *Privacy and Security Enforcement: Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last accessed Apr. 8, 2024).

time monitoring their credit and governmental communications guarding against identity theft, and resolving fraudulent claims and charges because of Defendants' actions and/or inactions.

**I. Plaintiffs and Class Members Suffered Additional Damages**

152. Plaintiffs and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

153. The ramifications of Defendants' disclosure and failure to keep individuals' PI secure are long lasting and severe. Once PI is disseminated to unauthorized parties, fraudulent use of that information and damage to victims may continue for years.[39]

154. Plaintiffs' and Class Members' driver's license numbers are private, valuable, and sensitive in nature as they can be used to commit a lot of different harms and fraud in the hands of the wrong people. Defendants did not obtain Plaintiff's and Class Members' consent to disclose such PI to any other person, as required by applicable law and industry standards.

155. Defendants' decision to expose Plaintiffs and Class Members to the possibility that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's driver's license number by utilizing Defendants' front-facing online instant quote platform left Plaintiffs and Class Members with no ability to protect their sensitive and private PI.

156. Defendants had the resources necessary to prevent their Data Disclosure, but did not implement data security measures, despite their obligations to protect Plaintiffs' and Class Members' PI from unauthorized disclosure.

157. Defendants failed to take reasonable steps to adequately secure Defendants' website and publish it in a manner that did not hand over Plaintiffs' and Class Members' driver's

[39] LEXISNEXIS RISK SOLUTIONS, *True Cost of Fraud Studies*, https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (last visited Apr. 8, 2024).

license numbers to unauthorized third parties, leaving Defendants' customers and other consumers, including Plaintiffs and Class Members, exposed to risk of fraud and identity theft.

158. Defendants were, and at all relevant times have been, aware that the PI they handle and store in connection with their services is highly sensitive. Because Defendants are companies that provide insurance services involving highly sensitive and identifying information, Defendants were aware of the importance of safeguarding that information and protecting their websites, systems, and products from security vulnerabilities.

159. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and they were alerted to the risk associated with knowingly providing driver's license numbers to members of the public on Defendants' website.

160. Defendants knowingly obtained, used, disclosed, and compromised Plaintiffs' and Class Members' PI by creating the Quote Platform with an auto-populate feature, voluntarily transmitting PI to any member of the public, including fraudulent actors. Defendants failed to take reasonable steps against an obvious threat. Defendants designed and implemented their own website, which included the instant quote feature that auto-populated Plaintiffs' and Class Members' driver's license numbers in response to the input of basic publicly available consumer information, was a feature that Defendants knowingly and intentionally included on their website. Had Defendants never used the information to sell auto insurance or never included this feature on their sales platform, they would have prevented the disclosure, unauthorized access, and ultimately, the prospective fraudulent use and possible fraudulent use of consumers' PI.

161. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would

have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of Defendants' Data Disclosure on their lives.

162. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[40]

163. As a result of Defendants' Data Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at imminent risk of suffering:

a. The compromise, publication, fraudulent, and/or unauthorized use of their PI,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and wages and loss of productivity associated with efforts expended from addressing and attempting to mitigate the actual and future consequences of Defendants' Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PI, which remains in the possession of Defendants and is subject to further compromise so long as Defendants fail to undertake appropriate measures to protect the PI in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of Defendants' Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

164. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further disclosure, misappropriation, and theft.

---

[40] U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS BUREAU OF JUSTICE STATISTICS, *Victims of Identity Theft 2012*, https://www.icpsr.umich.edu/web/NACJD/studies/34735/datadocumentation (last accessed Apr. 8, 2024).

165. To date, other than providing 12 months of credit monitoring and identity protection services, Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to do the following:

- "be vigilant for incidents of fraud or identity theft"
- "review[] [their] account statements and credit reports for any unauthorized activity"
- obtain a copy of their free credit report
- contact the FTC and/or the state Attorney General's office to report misuse of their personal information
- obtain additional information about avoiding identity theft

None of these recommendations, however, requires Defendants to expend any effort to protect Plaintiffs' and Class Members' PI; moreover, they fail to provide monetary compensation and provide no protection whatsoever after 12 months.

166. Defendants' disclosure of Plaintiffs' and Class Members' driver's license numbers directly to members of the public with small amounts of their PI has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Indeed, as Defendants' Notice indicates, they are putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

167. Defendants' offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come.

168. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen PI for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

169. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI is acquired and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

170. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, because of Defendants' Data Disclosure and the fact that their driver's license numbers are now in the hands of criminals, including but not limited to: invasion of privacy; loss of privacy; loss of control over PI and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PI; harm resulting from damaged credit scores and credit information; a substantially increased risk of future identity theft and fraud; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized disclosure of PI.

## V. CLASS ALLEGATIONS

171. Plaintiffs bring this action on behalf of themselves and the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**: All residents of the United States whose driver's license numbers and other PI was obtained, used, and/or disclosed by Defendants through their Quote Platform or otherwise displayed on their website, including but not limited to during the Data Disclosure.

---

[41] *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, at 29, *see supra* at n.33 (emphasis added).

> **Massachusetts Class**: All residents of Massachusetts whose driver's license numbers and other PI was obtained, used, and/or disclosed by Defendants through their Quote Platform or otherwise displayed on their website, including but not limited to during the Data Disclosure.[42]

172. The above defined classes are collectively referred to as the "Class" or "Classes." Plaintiffs reserve the right to re-define the Class(es) prior to class certification. Plaintiffs reserve the right to modify these class definitions as discovery in this action progresses.

173. Excluded from the Class are Defendants and their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

174. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable, as the proposed Classes appear to include at least hundreds of thousands of members who are geographically dispersed.

175. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendants' uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

176. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests are aligned with the Classes they seek to represent and they have no conflicts of interest with the Classes. Plaintiffs' Interim Co-Lead Class Counsel are competent with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and Plaintiffs' Interim Co-Lead Class Counsel intend to

[42] This Class is brought on behalf of the MA Plaintiffs, only, and not Plaintiff Brule.

prosecute this action vigorously. The Classes' interests are well-represented by Plaintiffs and Plaintiffs' Interim Co-Lead Class Counsel.

177. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation also presents a potential for inconsistent or contradictory judgments. Individualized litigation further increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

178. **Commonality and Predominance**: The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. whether Defendants engaged in the wrongful conduct alleged herein;

b. whether Defendants knowingly used Plaintiffs' and the Class Members' driver's license numbers to promote and sell auto insurance;

c. whether Defendants knowingly disclosed Plaintiffs' and the Class Members' driver's license numbers;

d. whether Defendants violated the DPPA;

e. whether Defendants' data security practices and the vulnerabilities of Defendants' systems resulted in the disclosure of Plaintiffs' and other Class Members' sensitive information;

f. whether Defendants violated Plaintiffs' and the Class Members' privacy rights;

g. whether Defendants were negligent or negligent per se when they disclosed the sensitive information of Plaintiffs and other Class Members; and

h. whether Plaintiffs and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

179. Given that Defendants engaged in a common course of conduct as to Plaintiffs and the Classes, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

## VI. CAUSES OF ACTION

### COUNT I
### Violation of the Driver's Privacy Protection Act, 18 U.S.C. §§ 2724, *et seq.*
### (On Behalf of Plaintiffs and the Nationwide Class or, in the alternative, by the MA Plaintiffs on behalf of the Massachusetts Class)
### (Against All Defendants)

180. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

181. Plaintiffs bring this claim individually and on behalf of the Nationwide Class, or in the alternative, the by the MA Plaintiffs on behalf of the Massachusetts Class.

182. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains. . . ." 18 U.S.C. § 2724.

183. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

184. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). Driver's license numbers are motor vehicle records and "personal information" under the DPPA. 18 U.S.C. § 2725(3).

185. Defendants obtain, use, and disclose motor vehicle records from their customers.

186. Defendants also obtain motor vehicle records directly from state agencies or through resellers (third party prefill services) who sell such records.

187. Defendants knowingly used the above described information to sell auto insurance on their free online Quote Platform, accessible from www.mapfreinsurance.com.

188. Defendants knowingly published the above described information to the public on their free online Quote Platform, accessible from www.mapfreinsurance.com.

189. Defendants knowingly linked their respective public websites to systems and/or networks storing maintaining, and/or obtaining Plaintiffs' and Class Members' PI.

190. Defendants had a practice of offering online insurance quotes to applicants long before they incorporated this auto-population feature, but added the auto-population feature to their online Quote Platform in order to gain competitive advantage in their sales process. By adding the auto-population feature to their online Quote Platform, which Defendants knowingly chose to do, Defendants knew that they were using the driver's license information to sell insurance and making the displayed information easily accessible to anyone who entered basic information into their system. Defendants did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. Defendants did not impose effective security protocols to prevent automated bots from accessing consumers' PI.

191. During the time period up until, at earliest, July 2023, PI, including driver's license numbers, of Plaintiffs and Class Members, were publicly available and viewable on Defendants' Quote Platform, and Defendants knowingly obtained, used, and disclosed and/or redisclosed Plaintiffs' and Class Members' motor vehicle records and PI to the general public, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

192. Pursuant to the allegations herein, Defendants knew or should have known that they obtained, disclosed or re-disclosed, and used PI from a motor vehicle record for a purpose not permitted under the DPPA.

193. By engaging in the conduct described above, Defendants knowingly obtained personal information for a purpose not permitted under the DPPA.

194. By engaging in the conduct described above, Defendants knowingly used personal information for a purpose not permitted under the DPPA.

195. By engaging in the conduct described above, Defendants knowingly disclosed or re-disclosed personal information for a purpose not permitted under the DPPA.

196. As a result of Defendants' acquisition, use, subsequent Data Disclosure, and violations of the DPPA, Plaintiffs and putative Class Members are entitled to statutory damages to maximum allowable, actual damages, liquidated damages, and attorneys' fees and costs.

**COUNT II**
**Negligence**
**(On Behalf of Plaintiffs and the Nationwide Class**
**or, in the alternative, by the MA Plaintiffs on behalf of the Massachusetts Class)**
**(Against All Defendants)**

197. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

198. Plaintiffs bring this claim individually and on behalf of the Nationwide Class, or in the alternative, the by the MA Plaintiffs on behalf of the Massachusetts Class.

199. Defendants owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing their data security

systems to ensure Plaintiffs' and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

200. Defendants owed a duty to Plaintiffs and the Class Members to adopt, implement, and maintain a process by which they could detect vulnerabilities in their websites and systems in a reasonably expeditious period of time and to give prompt notice in the case of a data security incident, including an unauthorized use of data knowingly disclosed on Defendants' website.

201. Defendants owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that their systems and networks—and the personnel responsible for them—adequately protected PI it stored, maintained, used, accessed, and/or obtained.

202. Defendants further assumed the duty to implement reasonable security measures as a result of their general conduct, internal policies, and procedures, in which MAPFRE states, among other things, that Defendants "always made it a priority to protect your personal and privileged information"; "We limit access to your personal and privileged information to those persons who need to know it to perform their jobs and to provide service to you, and as required or permitted by law"; "We maintain physical and electronic safeguards to protect such information from unauthorized use or disclosure"; "We maintain physical, electronic, and procedural safeguards to secure your personal information."[43] Through these and other statements, Defendants specifically assumed the duty to comply with industry standards in protecting their customers' and other consumers' PI; and to adopt, implement, and maintain internal standards of data security that met those industry standards.

[43] MAPFRE INSURANCE, https://www.mapfreinsurance.com/privacy-policy/ (last accessed Apr. 8, 2024).

203. Defendants owed a duty by, on information and belief, entering into an Agreement for Access to Records and Data Maintained by the [Massachusetts] Registry of Motor Vehicles, which required them to certify that they will not use motor vehicle records' "information for any purpose not permitted under Massachusetts or Federal laws, rules or regulations … including the … DPPA … [and] the Standards for the Protection of Personal Information of Residents of the Commonwealth … and will comply with such laws and Order and all other applicable laws, state or federal, regarding access to and the use of motor vehicle records, personal information and data privacy and protection."[44] Defendants also agreed that "Personal Information accessed under this Agreement shall not be used to create or aggregate the data for any purpose, except as specifically provided by federal or state law or other sections of this Agreement."

204. Unbeknownst to Plaintiffs and Class Members, they were entrusting Defendants with their PI when Defendants obtained their PI from motor vehicle records directly from state agencies or through resellers or third party prefill services who sell such records. Defendants had an obligation to safeguard Plaintiffs' and Class Members' PI and were able to protect against the harm suffered by Plaintiffs and Class Members. Instead, Defendants chose to disclose Plaintiffs' and Class Members' driver's license numbers so they could sell more auto insurance.

205. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having their systems auto-populate online quote requests with private PI without the consent or authorization of the person whose PI was being provided. Only Defendants were in a position to ensure that their systems were sufficient to protect

[44] *See* COMM. OF MASS., "Agreement for Access to Records and Data Maintained by the Registry of Motor Vehicles," available at https://www.mass.gov/doc/dvs-packet-for-access/download (last accessed Apr. 8, 2024).

against harm to Plaintiffs and the Class resulting from a data security incident, instead they chose to disclose Plaintiffs' and Class Members' driver's license numbers so they could sell more auto insurance.

206. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendants' misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent disclosure of PI, and instead chose to disclose Plaintiffs' and Class Members' driver's license numbers.

207. Defendants acknowledge their conduct created actual harm to Plaintiffs and Class Members because Defendants instructed them to monitor their accounts for fraudulent conduct and identity theft, and offered one year of credit monitoring.

208. Defendants knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PI and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

209. Because Defendants knew that their disclosure of sensitive PI would damage thousands of individuals, including Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

210. Defendants breached their duties to Plaintiffs and Class Members, and thus were negligent, by designing the Quote Platform and website so that it automatically provided Plaintiffs' and Class Members' driver's license information directly to members of the public, failing to recognize in a timely manner that Plaintiffs' and Class Members' PI had been disclosed, and failing to warn Plaintiffs and Class Members in a timely manner that their PI had been disclosed.

211. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

212. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and the Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the disclosure of their PI.

213. Neither Plaintiffs nor the other Class Members contributed to Defendants' Data Disclosure.

214. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or fraudulent use of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Defendants' Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or to which Defendants continue to have access) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PI.

215. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' PI.

216. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT III**
**Violation of Massachusetts General Laws, Chapter 93A**
**(by the MA Plaintiffs on Behalf of the Massachusetts Class)**
**(Against All Defendants)**

217. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

218. MA Plaintiffs bring this claim individually and on behalf of the Massachusetts Class.

219. This cause of action is brought on behalf of Plaintiffs Richard Ma and Fred Devereaux on behalf of themselves and the Massachusetts Class pursuant to M.G.L. c. 93A §§ 2 and 9. M.G.L. c. 93A §2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. c. 93A § 9 permits any consumer injured by a violation of M.G.L. c. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

220. Plaintiffs allege that Defendants committed unfair business acts and/or practices in violation of M.G.L. c. 93A §§ 2 and 9.

221. Defendants knew or should have known of the inherent risks in having their systems auto-populate online quote requests with private PI without the consent or authorization of the person whose PI was being provided. Only Defendants were in a position to ensure that their systems were sufficient to protect against harm to Plaintiffs and the Class resulting from a data

security incident, instead they chose to disclose Plaintiffs' and Class Members' driver's license numbers so they could sell more auto insurance.

222. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendants' misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent disclosure of PI, and instead chose to disclose Plaintiffs' and Class Members' driver's license numbers.

223. Defendants acknowledge their conduct created actual harm to Plaintiffs and Class Members because Defendants instructed them to monitor their accounts for fraudulent conduct and identity theft, and offered one year of credit monitoring.

224. Defendants knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PI and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

225. Defendants failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiffs' and Class Members' PI, failed to adequately monitor the security of Defendants' Quote Platform and website, knowingly provided Plaintiffs' and Class Members' driver's license information directly to members of the public with small amounts of their PI, failed to recognize in a timely manner that Plaintiffs' and Class Members' PI had been disclosed, and failed to warn Plaintiffs and Class Members in a timely manner that their PI had been disclosed.

226. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. c. 93A § 2.

227. As a direct and proximate result of Defendants' unfair acts and practices, Plaintiffs and the Massachusetts Class have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or fraudulent use of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Defendants' Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or to which Defendants continue to have access) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PI.

228. Neither Plaintiffs Ma and Devereaux, nor the other Massachusetts Class Members contributed to Defendants' Data Disclosure.

229. Plaintiffs Ma and Devereaux made a demand for relief, in writing, to Defendants at least thirty (30) days prior to filing this complaint, as required by M.G.L. c. 93A § 9. Plaintiffs

have not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Plaintiffs and the Massachusetts Class.

230. Based on the foregoing, Plaintiffs Ma and Devereaux and the other members of the Massachusetts Class are entitled to all remedies available pursuant to M.G.L c. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

231. Pursuant to M.G.L. c. 231, § 6B, Plaintiffs and other members of the Massachusetts Class are further entitled to pre-judgment interest as a direct and proximate result of Defendants' wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation and Plaintiffs and other members of the Massachusetts Class are entitled to interest in an amount according to proof.

**COUNT IV**
**Invasion of Privacy**
**(On Behalf of Plaintiffs and the Nationwide Class**
**or, in the alternative, by the MA Plaintiffs on behalf of the Massachusetts Class)**
**(Against All Defendants)**

232. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

233. Plaintiffs bring this claim individually and on behalf of the Nationwide Class, or in the alternative, the by the MA Plaintiffs on behalf of the Massachusetts Class.

234. General Laws c. 214, § 1B, inserted by St. 1974, c. 193, § 1, provides in relevant part: "A person shall have a right against unreasonable, substantial or serious interference with his privacy."

235. Plaintiffs' driver's license numbers and the other personally identifying

information obtained and disclosed by Defendants during the Data Disclosure was of a private, secluded and highly personal nature.

236. Defendants obtaining Plaintiffs' driver's license numbers and other personally information about Plaintiffs was an unreasonable, substantial, and serious invasion of Plaintiffs' privacy and constituted an intrusion on Plaintiffs' seclusion. Defendants had no legitimate basis to obtain Plaintiffs' private information.

237. Defendants' disclosure of Plaintiffs' driver's license numbers to nefarious third parties was an unreasonable, substantial, and serious invasion of Plaintiffs' privacy and constituted an intrusion on Plaintiffs' seclusion. Defendants had no legitimate basis to disclose Plaintiffs' private information to nefarious third parties.

238. As a result of Defendants' obtaining and disclosing their private information, Plaintiffs have suffered injuries and are entitled to compensation.

**COUNT V**
**Declaratory and Injunctive Relief**
**(On Behalf of Plaintiffs and the Nationwide Class**
**or, in the alternative, by the MA Plaintiffs on behalf of the Massachusetts Class)**
**(Against All Defendants)**

239. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

240. Plaintiffs bring this claim individually and on behalf of the Nationwide Class, or in the alternative, the by the MA Plaintiffs on behalf of the Massachusetts Class.

241. As previously alleged, Plaintiffs and Class Members have a reasonable expectation that companies such as Defendants, who could access their PI through automated systems, would provide adequate security for that PI.

242. Defendants owe a duty of care to Plaintiffs and Class Members requiring them to adequately secure PI.

243. Defendants still possess and can still access PI regarding Plaintiffs and Class Members.

244. Since their Data Disclosure, Defendants have announced few, if any changes to their decision to disclose the PI, their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems or Quote Platform.

245. Defendants' Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address the security failings that led to such exposure.

246. There is no reason to believe that Defendants' security measures are more adequate now to meet Defendants' legal duties than they were before their Data Disclosure.

247. Plaintiffs therefore seeks a declaration (1) that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) that to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendants not to disclose PI, including driver's license information, to the general public through their website or sales platforms;

b. Ordering Defendants to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated inquiries by bots, simulated cyber-attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

c. Ordering Defendants to engage third–party security auditors and internal personnel to run automated security monitoring, including risk analysis on Defendants' decision making,

d. Ordering Defendants to audit, test, and train their security personnel regarding any new or modified procedures,

e. Ordering Defendants not to make PI available on their Quote Platform,

f. Ordering Defendants not to store PI or make PI accessible in any publicly facing website,

g. Ordering Defendants to purge, delete, and destroy in a reasonably secure manner customer and consumer data not necessary for their provisions of services,

h. Ordering Defendants to conduct regular computer system scanning and security checks; and

i. Ordering Defendants routinely and continually to conduct internal training and education to inform employees and officers on PI security risks, internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a data security incident.

## VII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Classes, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as the class representatives and Plaintiffs' Interim Co-Lead Class Counsel as class counsel;

B. Award Plaintiffs and Class Members actual, statutory, punitive, monetary, and nominal damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

## VIII. JURY TRIAL DEMANDED

Plaintiffs hereby demands a trial by jury on all issues so triable.

Dated: April 8, 2024

Respectfully submitted,

*/s/ E. Michelle Drake*

E. Michelle Drake (admitted *pro hac vice*)
**BERGER MONTAGUE PC**
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5999
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto (admitted *pro hac vice*)
**BERGER MONTAGUE PC**
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

*/s/ Jason S. Rathod*

Jason S. Rathod (admitted *pro hac vice*)
Nicholas A. Migliaccio (admitted *pro hac vice*)
Bruno Ortega-Toledo (*pro hac vice* forthcoming)
**MIGLIACCIO & RATHOD LLP**
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
jrathod@classlawdc.com
nmigliaccio@classlawdc.com
bortega@classlawdc.com

Robert Ahdoot (*pro hac vice*)
*rahdoot@ahdootwolfson.com*

Alyssa Brown (*pro hac vice* to be filed)
*abrown@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Andrew W. Ferich (*pro hac vice*)
*aferich@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Stephen J. Teti (BBO # 569332)
**LOCKRIDGE GRINDAL NAUEN PLLP**
265 Franklin Street, Suite 1702
Boston, MA 02110
Telephone: (612) 339-6900
Email: sjteti@locklaw.com

Karen Hanson Riebel (admitted *pro hac vice*)
Kate M. Baxter-Kauf (admitted *pro hac vice*)
Emma Ritter Gordon (*pro hac vice*)
**LOCKRIDGE GRINDAL NAUEN P.L.L.P.**
100 Washington Ave. South, Suite 2200
Minneapolis, MN 55401-2159
Telephone: (612) 339-6900
Email: khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
erittergordon@locklaw.com

Gary F. Lynch (admitted *pro hac vice*)
Nicholas A. Colella (*pro hac vice* forthcoming)
Patrick D. Donathen (*pro hac vice* forthcoming)
**LYNCH CARPENTER, LLP**
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: 412-322-9243
Email: Gary@lcllp.com
NickC@lcllp.com
Patrick@lcllp.com

Joseph P. Guglielmo (Bar No. 671410)
Amanda M. Rolon (admitted *pro hac vice*)
Joseph G. Cleeman (admitted *pro hac vice*)
**SCOTT+SCOTT ATTORNEYS AT LAW LLP**
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
arolon@scott-scott.com
jcleeman@scott-scott.com

Patrick J. Sheehan (BBO# 639320)
**WHATLEY KALLAS LLP**
101 Federal Street, 19th Floor
Boston, Massachusetts 02110
Telephone: (617) 203-8459
Facsimile: (800) 922-4851
psheehan@whatleykallas.com

DAVID PASTOR (BBO 391000)
dpastor@pastorlawoffice.com
**PASTOR LAW OFFICE PC**
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617.742.9700
Fax: 617.742.9701

*Counsel for Plaintiffs*

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the CM/ECF system on April 8, 2024 will be sent electronically to the registered participants as identified on the Notice of Electronic Filing, which includes counsel for all parties.

*/s/ E. Michelle Drake*
E. Michelle Drake, *pro hac vice*